CLAIMS:

1. A circuit arrangement (100) for electronic data processing

- having at least one non-volatile memory module (10) for storing data to be protected against unauthorized access by means of encryption or decryption;

- having at least one memory module interface logic circuit (12) assigned to the memory module (10)

-- for addressing the memory module (10) and

-- for writing the data to the memory module (10) or

-- for reading out the data from the memory module (10);

- having at least one code R[ead]O[nly]M[emory] module (20) for storing and/or supplying at least one R[ead]O[nly]M[emory] code; and

- having at least one code ROM module interface logic circuit (22) assigned to the code ROM module (20)

-- for addressing the code ROM module (20) and

-- for reading out the ROM code from the code ROM module (20),

characterized in that at least one key code for encrypting or decrypting the data assigned to the memory module (10) may be extracted and/or generated from the at least one ROM code of the code ROM module (20).

2. A circuit arrangement as claimed in claim 1, characterized in that the memory module interface logic circuit (12) comprises at least one en-/decryption logic circuit (14)

- having at least one key address generation unit (16) and

- having at least one key register (18).

3. A circuit arrangement as claimed in claim 1 or 2, characterized in that the code ROM module interface logic circuit (22) comprises at least one multiplexing unit (24).

4. A circuit arrangement as claimed in at least one of claims 1 to 3, characterized in that the memory module (10) takes the form of

- at least one E[rasable] P[rogrammable]R[ead]O[nly]M[emory],

- at least one E[lectrical]E[rasable] P[rogrammable]R[ead]O[nly]M[emory] or
- at least one Flash memory.

5. A microcontroller, in particular an "embedded security controller", comprising at least one circuit arrangement as claimed in at least one of claims 1 to 4.

6. A method of encrypting or decrypting data to be protected against unauthorized access in at least one non-volatile memory module (10), characterized in that the data assigned to the memory module (10) are encrypted or decrypted by means of at least one ROM code supplied by at least one code R[ead]O[nly]M[emory] module (20).

7. A method as claimed in claim 6. characterized in that the key code serving in encryption or decryption is generated

- by reading out the ROM code in parallel with at least one access to the memory module (10), i.e. in parallel with at least one write operation or read operation of the memory module (10) or
- by one-off reading out of particular ROM code bytes, in particular at the time of the reset sequence, and by storing these ROM code bytes in at least one key register (18) until the time of at least one access to the memory module (10), i.e. until these ROM code bytes are required for at least one write operation or read operation of the memory module (10).

8. A method as claimed in claim 6 or claim 7, characterized in that,

- on access to the memory module (10) by means of at least one memory module address coming from at least one C[entral]P[rocessing]U[nit], at least one ROM key address is generated,
- the ROM code is fetched from the code ROM module (20) by means of the ROM key address and
- the ROM code is used as at least one en-/decryption key for encryption or decryption
  - -- of the address of the memory module (10) and/or
  - -- of the data to be written to the memory module (10) or
  - -- of the data to be read out from the memory module (10).

9. A method as claimed in at least one of claims 6 to 8, characterized in that
- the address of the memory module (10) and/or
- the data to be written to the memory module (10) or
- the data to be read out from the memory module (10)

are scrambled by means of at least one scrambling logic circuit.

10. Use of at least one circuit arrangement (100) as claimed in at least one of claims 1 to 4 in at least one chip unit, in particular in at least one "embedded security controller".